



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/923,213	08/06/2001	Lynn Henry Wheeler	10399-34384	8986

26702 7590 02/21/2006

MORRIS, MANNING & MARTIN LLP  
1600 ATLANTA FINANCIAL CENTER  
3343 PEACHTREE ROAD NE  
ATLANTA, GA 30326

EXAMINER

SCHUBERT, KEVIN R

ART UNIT PAPER NUMBER

2137

DATE MAILED: 02/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/923,213

Applicant(s)

WHEELER ET AL.

Examiner

Kevin Schubert

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 07 February 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-5 and 21-31 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-5 and 21-31 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

**DETAILED ACTION**

Claims 1-5 and 21-31 have been considered.

***Double Patenting***

5           The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982);  
10 *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

          A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37  
15 CFR 1.130(b).

          Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

20           Claims 1-5 and 21-31 of the instant application are rejected by U.S. Patent No. 6,915,430, U.S. Patent No. 6,892,302, copending U.S. Patent Application No. 10/248,626, and copending U.S. Patent Application No. 10/248,629. A discussion of how independent claim 1 is met by each of the four cases is cited below. The examiner notes that the dependent claims are met by the four cases as well but haven't been specifically discussed for the sake of brevity.

25           Claims 17 of U.S. Patent No. 6,915,430 contains every element of claim 1 of the instant application and as such anticipates claim 1 of the instant application. Claim 18 of U.S. Patent No. 6,892,302 contains every element of claim 1 of the instant application and as such anticipates claim 1 of the instant application. Claim 28 of copending U.S. Patent Application No. 10/248,626 contains every element of claim 1 of the instant application and as such anticipates claim 1 of the instant application.  
30           Claim 35 of copending U.S. Patent Application No. 10/248,629 contains every element of claim 1 of the instant application and as such anticipates claim 1 of the instant application.

          "A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or anticipated by, the earlier claim. *In re Longi*, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over

Art Unit: 2137

claims in four prior art patents); In re Berg, 140 F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness-type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species within that genus)." Eli Lilly and Company v Barr Laboratories, Inc., United States Court of Appeals for the Federal Circuit, On Petition for Rehearing en Banc (Decided: May 30, 2001).

***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

10       The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

15       Applicant has added the limitation "by storing the public key in association with the other information in a database". The meaning of this phrase is not definitive. Specifically, it is unclear whether the public key AND the other information are stored in a database or whether the public key (which happens to be in association with other information) is only stored in the database. Appropriate correction is required.

20       Claim 24 recites the limitation "the unique account identifier". There is insufficient antecedent basis for this limitation in the claim.

Claim 25 recites the limitation "the PuK-linked information maintained in the database for each user". There is insufficient antecedent basis for this limitation in the claim.

25       Claim 26 recites the limitation "the user-specific information". There is insufficient antecedent basis for this limitation in the claim.

Art Unit: 2137

Claims 26-28 are rejected under 112, second paragraph, for improper dependence. Claims 26-27 recite the limitation the method of claims 12 and 6, respectively. Examiner respectfully notes that both claim 12 and claim 6 are cancelled claims. Claim 28 is rejected accordingly for its dependence on claim 27.

5

Claim 29 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicant refers to "the public key associated with the account" in part b. Prior to this reference, applicant has disclosed at least two separate public keys associated with an account (i.e. a public key in a public-private key pair created within a secure environment and a new key). Accordingly, it is unclear which public key applicant is referring to.

10

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

15

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

20

Claims 1,4-5,21, and 25 are rejected under 35 U.S.C. 102(b) as being anticipated by Fischer, U.S. Patent No. 5,422,953.

25

As per claim 1, the applicant describes a method of manufacturing devices comprising the following limitations which are met by Fischer:

a) creating a public-private key pair within the secured environment, the private key for utilization in generating a digital signature for an electronic message, the public key exportable for use by third parties in connection with authenticating the electronic message (Col 4, lines 29-34; Fig 2);

Art Unit: 2137

b) storing the private key within the device against the possibility of divulgement thereof by the device (Col 4, lines 29-34; Col 6, lines 10-65);

c) securely linking the public key with other information by storing the public key in association with the other information in a database within the secure environment (Col 2, lines 19-37, Col 6, lines 10-65).

As per claim 4, the applicant describes the method of claim 1, which is met by Fischer, with the following limitation which is also met by Fischer:

Wherein the other information comprises respective security features and a manufacturing history of each device (Fischer: Col 6, lines 10-65).

As per claim 5, the applicant describes the method of claim 2, which is met by Fischer, with the following limitation which is also met by Fischer:

Further comprising identifying a particular manufactured device by authenticating a message using one of said linked public keys, a digital signature for the message having been generated by the particular manufactured device (Fischer: Col 7, lines 20-34).

As per claim 21, the applicant describes the method of claim 1, which is met by Fischer, with the following limitation which is also met by Fischer:

Wherein the public key and information linked therewith is obtained from a secure entity (Col 4, lines 29-34).

As per claim 25, the applicant describes the method of claim 1, which is met by Fischer, with the following limitation which is also met by Fischer:

Wherein the PuK-linked information maintained in the database for each user further includes user-specific information (Col 2, lines 19-37).

Art Unit: 2137

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 2-3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer in view of Spies, U.S. Patent No. 6,230,269.

As per claim 2, the applicant describes the method of claim 1, which is met by Fischer, with the following limitation which is met by Spies:

Wherein each private-public key pair is created within each device based on a random number produced by a random number generator disposed within each device (Spies: claim 16);

Fischer discloses all the limitations of claim 1. Fischer even discloses the use of a random number generator. However, Fischer does not specifically disclose that the public-private key pair is produced using the random number generator.

Spies discloses a public-private key pair being produced from a random number generator. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Spies with those of Fischer because using a random number generator to produce a key pair ensures freshness of the key pair.

As per claim 3, the applicant describes the method of claim 2, which is met by Fischer in view of Spies, with the following limitation which is met by Fischer:

Wherein each digital signature generated by each device is a random number (Fischer: Col 4, lines 2-7).

Art Unit: 2137

Claims 22-24 and 27-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer in view of Ramasubramani, U.S. Patent No. 6,233,577.

5           As per claim 22, the applicant describes the method of claim 1, which is met by Fischer, with the following limitation which is met by Ramasubramani:

Wherein the PuK-linked information stored in the database includes the identity of a plurality of third-parties with which an account is maintained, the accounts being identified by one of a plurality of third-party account identifiers (Ramasubramani: Fig 4B);

10           Fischer discloses all the limitations of claim 22. However, Fischer does not disclose storing in the database the identity of a plurality of third-parties with which an account is maintained, the accounts being identified by one of a plurality of third-party account identifiers.

This idea is disclosed by Ramasubramani in a system in which certificates are stored and maintained for a plurality of third-parties in a centralized database, the accounts being identified by one of  
15 a plurality of third-party account identifiers. Combining Ramasubramani allows for centralized storage of certificates for a plurality of third-parties. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Ramasubramani with those of Fischer because doing so makes the system more robust and efficient by allowing for centralized storage and retrieval of certificates for a plurality of users.

20

As per claims 23-24 and 27-28, the applicant describes the method of claim 22, which is met by Fischer in view of Ramasubramani, with the following limitation which is met by Ramasubramani:

Wherein the PuK-linked account information of the users is indexed in the database by unique account identifiers such that the PuK-linked account information for a user is retrieval from the database  
25 based on the account identifier (Ramasubramani: Fig 4B).



Art Unit: 2137

Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer in view of Schneier (Schneier, Bruce. Applied Cryptography. John Wiley & Sons. 1996. pages 185-187).

As per claim 26, the applicant describes the method of claim 12, which is a cancelled claim, with the following limitation which is met by Schneier:

Wherein the user-specific information includes the name and address of the user (Schneier: page 186).

Claim 26 depends on claim 12, which is cancelled, and claim 26 recites the limitation "the user-specific information" which appears to have a lack of antecedent basis issue as well. In the event applicant intends claim 26 to depend on a claim met by the Fischer or the Fischer in view of Ramasubramani system, Examiner submits that Fischer alone or taken in combination with Ramasubramani disclose the user of user-specific information such as a certificate but are silent as to the information in the certificate. Schneier discloses the well-known idea that a certificate may disclose the name and address of a user.

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Schneier with Fischer (or Fischer in view of Ramasubramani) and include the name and address of a user for further identification purposes.

Claims 29-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer in view of Menezes (Menezes, Alfred J. Handbook of Applied Cryptography. CRC Press. 1997. pages 25-32; 546-548; 572-577).

As per claim 29, the applicant describes the method of claim 1, which is met by Fischer, with the following limitations:

a) receiving an EC, the EC including an account identifier and a message including the new public key and a digital signature therefor (Fischer: Col 2, lines 19-37);

Art Unit: 2137

b) authenticating the message of the EC using the public key associated with the account in the database identified by the account identifier, and upon successful authentication thereof (Menezes: pages 25-26);

c) sending an EC to each of the third-parties, each EC including the new public-key and the third-party account identifier for the respective third-party maintained in the database and associated with the account identified by the account identifier (Menezes: page 576);

Fischer discloses all the limitations of claim 1. Fischer does not disclose authenticating a message of the EC using the public key associated with the account in the database identified by the account identifier or sending an EC to each of the third-parties maintained in the database and associated with the account identified by the account identifier. Both of these limitations are met by Menezes.

Menezes discloses use of public-key cryptography in which a message is authenticated using an associated public key. Menezes also discloses use of a certificate directory in which certificates of users are maintained in a database. An EC, which may include a certificate, may be sent to each of the third-parties upon certificate creation or periodically. Combining the ideas of Menezes with those of Fischer provides many benefits for the system, including authentication of a user EC. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Menezes with those of Fischer because doing so provides a number of benefits to the system, including making the system more robust and secure by providing for authentication of a user message.

As per claim 30, the applicant describes the method of claim 29, which is met by Fischer in view of Menezes, with the following limitation which is met by Fischer:

Further comprising the step of digitally signing a message involving the new public key of the user and a third-party account identifier (Fischer: Col 2, lines 19-37).

As per claim 31, the applicant describes the method of claim 29, which is met by Fischer in view of Menezes, with the following limitation which is met by Menezes:

Art Unit: 2137

Further comprising the step of sending the EC received from the user to each of the third-parties (Menezes: page 576).

### ***Response to Arguments***

5           Applicant's remarks with respect to Examiner's submission that an exorbitant amount of prior art has been filed on numerous Information Disclosure Statements (IDS) have been noted. Examiner further notes his appreciation of Applicant's efforts.

10           Applicant's arguments, see Remarks filed 2/7/06, have been fully considered but they are not persuasive. In the previous action, Examiner made a double-patenting rejection based on the claims of the instant application being in conflict with claims of four other applications. Applicant appears to be in agreement with Examiner that a Terminal Disclaimer should be filed with respect to application numbers 10/248,625, 10/248,627, and 10/248,626. However, it appears that Applicant has filed no such Terminal Disclaimer. Accordingly, the double-patenting rejection with respect to these three applications has not  
15   been overcome.

          With regard to the double-patenting rejection with respect to application number 10/248,629, Applicant appears to traverse on the grounds that application number 10/248,629 contains additional functionality and based on this difference the claims are non-obvious variations of each other. Examiner respectfully disagrees with such an argument. It is respectfully submitted that the test for obvious-type  
20   double patenting is not whether the claims of a related application contain additional functionality. The test is whether the instant application is anticipated by, or obvious over, a related application. See *In re Longi*, 759 F.2d at 896, 225 USPQ at 651. Accordingly, applicant's arguments that related application 10/248,629 is patentably distinct because it contains additional functionality does not overcome the rejection.

25

Applicant's arguments with respect to the 102(b) rejection of claim 1 have been fully considered but they are not persuasive. Applicant presents the following argument:

Art Unit: 2137

(1) Fischer does not disclose "storing the public key in association with the other information in a database"

Examiner respectfully disagrees with the above. Fischer discloses a system in which a  
5 private/public key pair is created. Further, a public key is matched with the private key in the secure  
device. Specifically, a certificate issued by the device manufacturer associating the public key with the  
trusted device may be utilized. In effect, the user's certifier vouches that the device contains the user's  
private key. This embodiment allows each public key to accompany one certificate (Col 6, lines 24-32).  
Furthermore, **"certificates may be stored externally to the device (e.g. in storage associated with a  
10 computer driving the notary device) or internally"** (Col 2, lines 32-35).

From at least the above, Fischer discloses "storing the public key in association with other  
information in a database". Accordingly, the rejection is maintained.

Applicant's arguments with respect to claim 2 fail to comply with 37 CFR 1.111(b) because they  
15 amount to a general allegation that the claims define a patentable invention without specifically pointing  
out how the language of the claims patentably distinguishes them from the references. Specifically,  
Applicant notes a statement on what he is not claiming and then notes a statement on what he is  
claiming. Such an argument amounts to a general allegation as it does not indicate how the claims define  
a patentable invention by *specifically pointing out how the language of the claims patentably distinguishes  
20 them from the references.*

Applicant's arguments with respect to claim 3 have been fully considered but are not persuasive.  
Applicant argues that a digital signature, disclosed by Fischer in view of Spies, is not a random number.  
Examiner respectfully disagrees with the previous, for at least the reason that a digital signature is a  
25 random number.

Furthermore, Examiner fails to see how Applicant's argument is anything but spurious. The  
applied combination of Fischer in view of Spies is such that a private-public key pair generated from a

Art Unit: 2137

random number is used to create a digital signature output. Likewise, the claimed invention is such that a private-public key pair generated from a random number is used to create a digital signature output. An argument that the two outputs, created through a commensurate process, are antagonistic of each other appears to lack any justification.

5

Applicant's arguments with respect to claims 4 and 5 have been considered but are moot in view of the new ground(s) of rejection.

### ***Conclusion***

10 Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date  
15 of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX  
MONTHS from the date of this final action.

20 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where  
25 this application or proceeding is assigned is 571-273-8300.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should  
5 you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KS

10

  
EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER

15

20